UNITED STATES COURT OF APPEALS
Tenth Circuit
Byron White United States Courthouse
1823 Stout Street
Denver, Colorado 80294
(303) 844-3157

Patrick J. Fisher, Jr.
Clerk

Elisabeth A.Shumaker
Chief Deputy Clerk

May 13, 1997

TO: All recipients of the captioned opinion

RE: 95-6245, Davis v. Gracey
April 21, 1997

Please be advised of the following correction to the captioned decision:

In the attorney designation section on the first page, the first name of Michael Salem, counsel for Plaintiffs-Appellants, is spelled incorrectly. On the top of page two, the designation of counsel for Defendants-Appellants should reflect her current married name, Stacey Haws Felkner.

Please make the appropriate corrections.

Very truly yours,

Patrick Fisher, Clerk

Susie Tidwell
Deputy Clerk

F I L E D
United States Court of Appeals
Tenth Circuit

APR 21 1997

PATRICK FISHER
Clerk

PUBLISH

UNITED STATES COURT OF APPEALS
TENTH CIRCUIT

ANTHONY A. DAVIS, individually and doing business as Mid-America Digital Publishing Company, doing business as Oklahoma Information Exchange; GAYLA DAVIS, and JOHN BURTON, individuals; TSI TELECOMMUNICATION SPECIALISTS, INC., an Oklahoma corporation, Plaintiffs-Appellants, v. ANTHONY GRACEY, MARK WENTHOLD, and GREGORY TAYLOR, Officers in their official capacities as Oklahoma City Police Officers and as individuals, Defendants-Appellees,	No. 95-6245

Appeal from the United States District Court
for the Western District of Oklahoma
(D.C. No. CIV-94-335-L)

Michael Salem, Salem Law Offices, Norman, Oklahoma (William R. Holmes, Norman, Oklahoma, with him on the brief), for Plaintiffs-Appellants.

Stacey Haws Felkner (Robert E. Manchester and Susan A. Knight, with her on the brief), of Manchester & Pignato, Oklahoma City, Oklahoma, for Defendants-Appellees.

Before **SEYMOUR**, Chief Judge, **BARRETT** and **LIVELY**,[*] Senior Circuit Judges.

SEYMOUR, Chief Judge.

[*]The Honorable Pierce Lively, Senior United States Circuit Judge for the Sixth Circuit, sitting by designation.

Anthony Davis operated a large computer bulletin board system in Oklahoma City. After Mr. Davis sold obscene CD-ROMs to an undercover officer, a warrant was obtained to search his business premises. During the execution of the warrant, police officers determined pornographic CD-ROM files could be accessed through the bulletin board and seized the computer equipment used to operate it. Following his criminal conviction and civil forfeiture of the computer equipment in state court proceedings, Mr. Davis, his related businesses, and several users of electronic mail (e-mail) on his bulletin board brought this action in federal court against the officers who executed the search, alleging that the seizure of the computer equipment, and e-mail and software stored on the system, violated several constitutional and statutory provisions. The district court granted summary judgment for the officers. We affirm.

I

Background

Mr. Davis operated the Oklahoma Information Exchange, a computer bulletin board system. Computer users could subscribe to the bulletin board, dial in using a modem, then use the system to send and receive messages via e-mail,

access the Internet, utilize on-line databases, and download or upload software. According to Mr. Davis, approximately 2000 subscribers used his bulletin board.

In April 1993, the Oklahoma City Police Department received an anonymous tip that Mr. Davis was selling obscene CD-ROMs from his business premises. On three different occasions, an undercover officer purchased "adult" CD-ROMs directly from Mr. Davis. During one of these visits, Mr. Davis mentioned to the officer that he operated a bulletin board, and that similar pornographic images could be accessed by dialing in to the bulletin board. The officer never actually saw the computer equipment used to operate the bulletin board. In his affidavit for a search warrant, the officer did not mention the possibility that a bulletin board was being operated on the premises, or the possibility that this bulletin board could be used to distribute or display pornographic images. A judge determined that two CD-ROMs acquired from Mr. Davis were obscene, and issued a warrant to search his business premises for pornographic CD-ROMs and "equipment, order materials, papers, membership lists and other paraphernalia pertaining to the distribution or display of pornographic material in violation of state obscenity laws set forth in O.S. Title 21-1024.1." Aplee. supp. app., vol. I at 45.

Several officers, including defendants Anthony Gracey and Mark Wenthold, conducted the search at Mr. Davis' business. During the search, the officers

discovered the bulletin board. Attached to it were CD-ROM drives housing sixteen CD-ROM discs, including four discs identified by Mr. Davis to the officers as containing pornographic material. The officers believed from the configuration of the bulletin board computers that the files accessible via the bulletin board included files from the four pornographic CD-ROMs. The officers called for assistance from officer Gregory Taylor, who was reputed to be more knowledgeable about computers than they were. He confirmed that the pornographic CD-ROMs could be accessed via the bulletin board. The officers seized the computer equipment used to operate the bulletin board, including two computers, as well as monitors, keyboards, modems, and CD-ROM drives and changers. The seizure of this computer equipment is the subject of the federal proceedings in this case.

At the time of the seizure, the computer system contained approximately 150,000 e-mail messages in electronic storage, some of which had not yet been retrieved by the intended recipients. The hard drive of the computer system also contained approximately 500 megabytes of software which had been uploaded onto the bulletin board by individual subscribers. Mr. Davis intended to republish this "shareware" on a CD-ROM for sale to the public. Mr. Davis had previously published three such compilations of shareware on CD-ROM.

Mr. Davis was convicted of several counts of possessing and distributing obscenity, and of using a computer to violate Oklahoma statutes. His conviction was upheld on appeal. Davis v. State, 916 P.2d 251, 254 (Okla. Crim. App. 1996). The State also obtained civil forfeiture of the computer equipment used to operate the bulletin board. State ex rel. Macy v. One (1) Pioneer CD-ROM Changer, 891 P.2d 600, 607 (Okla. Ct. App. 1994). Law enforcement officials have apparently disclaimed any interest in the materials in electronic storage, either for purposes of evidence or forfeiture.

Mr. Davis, Gayla Davis, John Burton, and TSI Telecommunications Specialists, Inc.,[1] filed the instant suit in federal court alleging claims under 42 U.S.C. § 1983 for violation of First and Fourth Amendment rights, and under the Privacy Protection Act (PPA), 42 U.S.C. §§ 2000aa - 2000aa-12, and the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2711. The crux of the complaint is that the seizure of the equipment was illegal because the warrant was not sufficiently particular and because the seized computer system contained e-mail intended for private subscribers to the bulletin board, and software intended for future publication by Mr. Davis. Plaintiffs contend these

[1]Gayla Davis was, at the time of the search, Mr. Davis' wife and co-owner of the Oklahoma Information Exchange bulletin board. TSI Telecommunications is a corporation owned by Anthony and Gayla Davis. The Davises and John Burton were users of the bulletin board.

stored electronic materials were outside the scope of the warrant, and are protected by several congressional enactments.

Original defendants in this suit included the City of Oklahoma City, the Oklahoma City Police Department, and several officers of the Oklahoma City Police Department who executed the search and seizure of the computer equipment. The municipal entities were dismissed from the case. Plaintiffs do not dispute that their only remaining claims are against the officers in their individual capacities. The district court entered summary judgment for the officers, holding that their reliance on a valid warrant entitled them to qualified immunity on the constitutional claims, and entitled them to the statutory good faith defenses contained in the PPA and ECPA.

II

Preliminary Issues

At the outset, we must note the narrow scope of our consideration of the issues before us.[2] We address here plaintiffs' arguments only to the extent they concern the legality of the initial seizure of the computer equipment and the

[2]Although plaintiffs have raised several new arguments on appeal, we dispose only of those arguments that were advanced in the district court in opposition to the officers' motion for summary judgment. See Bancamerica Commercial Corp. v. Mosher Steel of Kansas, Inc., 100 F.3d 792, 798-99 (10th Cir. 1996).

electronic material stored therein. Plaintiffs make repeated references in their briefs to the retention by law enforcement authorities of the stored electronic material, and the failure of such authorities to copy or return the material when requested to do so.[3] A failure timely to return seized material which is without evidentiary value and which is not subject to forfeiture may state a constitutional or statutory claim. Cf. FED. R. CRIM. P. 41 advisory committee's note to 1989 Amendment (stating that even when property is lawfully seized, "if the United States' legitimate interests can be satisfied even if the property is returned, continued retention would become unreasonable"); In re Search of Kitty's East, 905 F.2d 1367, 1375 (10th Cir. 1990) (same). However, plaintiffs have made no allegation that defendant officers are persons with authority to return materials once seized. The City and the Police Department have been dismissed from this action. We therefore do not consider any potential violations of plaintiffs' constitutional or statutory rights that derive from failure or delay in returning or copying materials once seized. We address only those claims arising out of the initial seizure of the computer equipment in question.

The officers assert that plaintiffs' claims are barred by collateral estoppel and res judicata arising out of the state court criminal and forfeiture proceedings.

[3]It is not clear from the record whether plaintiffs made a proper request for the return of the electronically stored materials, or only for the computer equipment generally. The latter was subject to forfeiture, and thus plaintiffs were not entitled to its return.

We "must give the same preclusive effect to state court judgments that those judgments would be given in the courts of the state in which the judgments were rendered." Comanche Indian Tribe of Oklahoma v. Hovis, 53 F.3d 298, 302 (10th Cir. 1995). Collateral estoppel only applies to issues actually and necessarily determined in the prior proceeding. Laws v. Fisher, 513 P.2d 876, 877 (Okla. 1973). The officers concede the earlier proceedings in state court did not resolve the statutory claims raised by plaintiffs. The Oklahoma Court of Criminal Appeals did not address the issues. The Oklahoma Court of Appeals addressing the civil forfeiture declined to determine if a claim was stated under the ECPA or PPA, holding only that if such claims existed they would not affect the legality of the computer equipment forfeiture. One (1) Pioneer CD-ROM Changer, 891 P.2d at 605-07. Moreover, collateral estoppel applies only to persons who were parties or in privity with parties to the prior proceeding. Laws, 513 P.2d at 877. Without deciding if other plaintiffs are estopped from asserting their various claims, at a minimum we are not persuaded the officers have established that Mr. Burton is in privity with Mr. Davis. Consequently, at least one plaintiff is able to assert each claim on appeal; for convenience we will refer throughout to plaintiffs collectively.

We address in turn each of the claims remaining in this appeal.[4]

[4]On appeal, plaintiffs do not pursue a distinct First Amendment claim, although (continued...)

III

Fourth Amendment

The officers claim they are entitled to qualified immunity on the constitutional claims. We review *de novo* the district court's grant of qualified immunity on summary judgment, viewing the evidence in the light most favorable to the nonmoving party. Romero v. Fay, 45 F.3d 1472, 1475 (10th Cir. 1995). "We analyze assertions of qualified immunity under a two-part framework: first we determine whether the plaintiff has asserted a violation of a constitutional or statutory right, and then we decide whether that right was clearly established such that a reasonable person in the defendant's position would have known that her conduct violated the right." Garramone v. Romo, 94 F.3d 1446, 1449 (10th Cir. 1996) (citing Siegert v. Gilley, 500 U.S. 226, 231 (1991)). "[T]he plaintiff must articulate the clearly established constitutional right and the defendant's conduct which violated the right with specificity." Romero, 45 F.3d at 1475. Once the plaintiffs have met this initial burden, "the defendant must demonstrate that no material issues of fact remain as to whether his or her actions were objectively reasonable in light of the law and the information he or she possessed at the

---

[4](...continued)
they do assert that First Amendment concerns animate Fourth Amendment jurisprudence and the statutory remedies provided in the Privacy Protection Act.

time." Coen v. Runner, 854 F.2d 374, 377 (10th Cir. 1988). If we determine that plaintiffs have failed to show the officers' conduct constituted a violation of a constitutional or statutory right, we need not address the other elements of the qualified immunity inquiry.

Plaintiffs assert that the warrant did not specifically authorize the seizure of the computer equipment and thus was unconstitutionally overbroad. They suggest the officers misled the magistrate in procuring the warrant. Even if the warrant authorized the seizure of the computer equipment, plaintiffs contend the warrant should not have been executed in a manner resulting in the incidental seizure of e-mail and other files stored on the hardware which were clearly outside the scope of the warrant. We address each of the contentions in turn.

A. The Warrant

We review *de novo* whether the warrant was overbroad under the Fourth Amendment. United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988). "The fourth amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a 'general, exploratory rummaging in a person's belongings.'" Voss v. Bergsgaard, 774 F.2d 402, 404 (10th Cir. 1985) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)). "The particularity requirement ensures that a search is confined in scope to particularly

described evidence relating to a specific crime for which there is demonstrated probable cause." Id. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192, 196 (1927).

We have stated that "[t]he test applied to the description of the items to be seized is a practical one," Leary, 846 F.2d at 600, and the language in warrants is to be read in a "common sense fashion," In re Search of Kitty's East, 905 F.2d at 1374. Thus, "'[a] description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized.'" Leary, 846 F.2d at 600 (quoting United States v. Wolfenbarger, 696 F.2d 750, 752 (10th Cir. 1982)) (internal quotation omitted). "As an irreducible minimum, a proper warrant must allow the executing officers to distinguish between items that may and may not be seized." Id. at 602. Moreover, "[e]ven a warrant that describes the items to be seized in broad or generic terms may be valid 'when the description is as specific as the circumstances and the nature of the activity under investigation permit.'" Id. at 600 (quoting United States v. Santarelli, 778 F.2d 609, 614 (11th Cir. 1985)).

Plaintiffs suggest that the warrant's failure to indicate explicitly that "equipment" encompassed computer equipment or electronics was a fatal defect. We do not agree. We ask two questions: did the warrant tell the officers how to separate the items subject to seizure from irrelevant items, and were the objects seized within the category described in the warrant? Here, we answer both of these questions in the affirmative. The warrant directed the officers to search for "equipment . . . pertaining to the distribution or display of pornographic material in violation of state obscenity laws set forth in O.S. Title 21-1024.1." Aplee. supp. app., vol. I, at 45. Computer equipment which fell into this category could be legally seized. Plaintiffs do not dispute that the bulletin board could be used for dial-in access to and copying of pornographic files from the loaded CD-ROMs. The seized computer equipment fell within the scope of the warrant.

Alternatively, plaintiffs argue that if the computer equipment was encompassed in the language of the warrant, the warrant was overly broad. We disagree. The description given in the warrant was sufficient to provide a meaningful limitation on the search, and was far narrower than those we have found lacking sufficient particularity. We have invalidated warrants for overbreadth where the language of the warrants authorized the seizure of "virtually every document that one might expect to find in a . . . company's office," including those with no connection to the criminal activity providing the

probable cause for the search. Leary, 846 F.2d at 602; see also Voss, 774 F.2d at 405. We have also held that an "unadorned reference to a broad federal statute does not sufficiently limit the scope of a search warrant." Leary, 846 F.2d at 602; see also United States v. Brown, 984 F.2d 1074, 1077 (10th Cir. 1993) (holding overbroad language authorizing a search for "other item which the officers determine or have reasonable belief is stolen"). Similarly, the Ninth Circuit found insufficiently particular a warrant which "authorized the seizure of virtually every document and computer file" at the target company. United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995). The court emphasized that the warrant "contained no limitations on which documents within each category could be seized or suggested how they related to specific criminal activity." Id.

The warrant here was confined to that equipment "pertaining to the distribution or display of pornographic material." Aplee. supp. app., vol. I at 45. This description included only that equipment directly connected to the suspected criminal activity, not a wide range of equipment used for purposes unrelated to the suspected criminal activity. Nor did it encompass all the equipment one might expect to find at a legitimate business. Furthermore, the criminal activity referenced in the warrant was very narrow, providing a ready guide to determine if a given item was one that might be the instrument or evidence of the criminal activity. The warrant was not overbroad.

Our approval of the particularity of the warrant is bolstered by the execution of the search itself. The officers did not conduct a general search of the premises. They left behind approximately 2000 CD-ROM discs that Mr. Davis represented to be of his own manufacture and non-pornographic in nature. There is no evidence the officers attempted to search or seize computer equipment that was not connected to the CD-ROM drives or the bulletin board. The executing officers consulted with a more expert officer to confirm that the computer equipment was in fact used to distribute or display pornographic material and therefore fell within the scope of the warrant. If the executing officers had flagrantly disregarded the limitations of the warrant, an otherwise constitutional warrant might have been transformed into a general search. United States v. Medlin, 842 F.2d 1194, 1199 (10th Cir. 1988). There is no indication of such behavior here.

B. The Warrant Application

Plaintiffs also infer that the magistrate was misled by the failure of the affidavit for the warrant to mention either the possible existence of the bulletin board, or the possible distribution of pornography via computer, when the

swearing officer knew of these possibilities. However, plaintiffs do not suggest the magistrate was unaware that "equipment . . . pertaining to the . . . display of pornographic material" contained on CD-ROM discs was likely to include computers and related accessories. Indeed, the affidavit informed the magistrate that the swearing officer viewed one of the obscene discs "on a computer with a CD-ROM drive." Aplee. supp. app., vol. I at 43.

Plaintiffs assert that because the officers knew about the bulletin board but did not include this knowledge in the affidavit supporting the warrant their reliance on the warrant could not be in good faith. "Only where the warrant application is so lacking in indicia of probable cause as to render official belief in its existence unreasonable . . . will the shield of immunity be lost." Malley v. Briggs, 475 U.S. 335, 344-45 (1986) (citing United States v. Leon, 468 U.S. 897, 923 (1984)). The warrant was amply supported by probable cause. Plaintiffs have offered no theory why a reasonable officer would believe that omitting mention of the bulletin board would vitiate the probable cause contained in the affidavit. Plaintiffs' argument reduces to the narrow claim that the warrant was invalid because the affidavit failed to recite that a computer system might also be configured to allow remote viewing of the pornographic material via a computer bulletin board. We decline to invalidate a warrant supported by probable cause simply because officers executing it suspect, and then discover, that the target of

the search has employed an unstated methodology for using the objects specified in the warrant for commission of the crime referenced in the warrant.

C. Incidental Seizure of Electronically Stored Materials

Plaintiffs appear to argue that even if the warrant authorized the seizure of the computer equipment, such a seizure was nonetheless illegal because of the concomitant incidental seizure of e-mail and software stored therein.[5] We can discern no doctrinal support for this proposition. The argument appears to draw its force from plaintiffs' efforts to distinguish between the computer hardware--the "container"--and its contents. They repeatedly urge that the seizure was unlawful because no probable cause was asserted to seize the contents independent of the probable cause asserted to seize the computer equipment. The question then is whether the incidental temporary seizure of stored electronic materials invalidated the seizure of the computer within which they were stored. We hold that it did not.

Plaintiffs' argument fails for the simple reason that the computer equipment was more than merely a "container" for the files; it was an instrumentality of the crime. In the typical case, the probable cause supporting seizure of a container is probable cause to believe that the container's contents include contraband or

[5]We consider below the similar issues raised by plaintiffs' statutory claim under the ECPA.

evidentiary material. Here, in contrast, the probable cause supporting the seizure of the computer/container related to the function of the computer equipment in distributing and displaying pornographic images, not to its function in holding the stored files. The fact that a given object may be used for multiple purposes, one licit and one illicit, does not invalidate the seizure of the object when supported by probable cause and a valid warrant.

We also note the obvious difficulties attendant in separating the contents of electronic storage from the computer hardware during the course of a search. Perhaps cognizant of the potential burdens of equipment, expertise, and time required to access, copy, or remove stored computer files, plaintiffs have not suggested any workable rule. In short, we can find no legal or practical basis for requiring officers to avoid seizing a computer's contents in order to preserve the legality of the seizure of the computer hardware.

In any event, we are well able to distinguish between the legality of the initial seizure of a container, and any subsequent search or retention of the contents. See, e.g., United States v. Corral, 970 F.2d 719, 725 (10th Cir. 1992); United States v. Donnes, 947 F.2d 1430, 1436 (10th Cir. 1991). Even in the typical case, seizure of a container need not be supported by probable cause to believe that *all* of the contents of the container are contraband. The seizure of a container is not invalidated by the probability that some part of its "innocent"

contents will be temporarily detained without independent probable cause. We will not hold unlawful the otherwise constitutional seizure of the computer equipment in order to prevent the temporary deprivation of plaintiffs' rights to the contents. However, our conclusion that the seizure of the computer equipment pursuant to a warrant here allowed the incidental seizure of files stored therein should not be read as approval of any subsequent efforts by the police to search or retain the stored files without a warrant.[6]

Finally, plaintiffs suggest that once the CD-ROMs and CD-ROM drives were seized, the officers lacked cause to remove the remainder of the computer equipment. Again, we are unable to discern a practical or doctrinal basis for this proposed rule of minimization. The computer equipment as a whole was an instrumentality of the crime of distributing obscenity, and the equipment was covered by the warrant.

Viewing the evidence in the light most favorable to plaintiffs, the conduct of the officers did not rise to a constitutional violation. The district court therefore properly granted summary judgment to the officers on plaintiffs' constitutional claim.

---

[6]Not only is there no evidence that the officers ever read the e-mail or files in question, the law enforcement personnel involved in this action repeatedly, both in state and federal court, disclaimed any interest in the contents thereof.

IV

Privacy Protection Act

Plaintiffs assert that the seizure of the stored electronic materials constituted a violation of the Privacy Protection Act (PPA), 42 U.S.C. §§ 2000aa - 2000aa-12. The PPA provides that

> it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of publication.

42 U.S.C. 2000aa(a).[7] The PPA requires law enforcement officers, absent exigent circumstances, id. § 2000aa(a)(2), to rely on subpoenas to acquire materials intended for publication unless "there is probable cause to believe that the person possessing [work product] materials has committed or is committing the criminal offense to which the materials relate," id. § 2000aa(a)(1).

The statute creates a civil cause of action for damages resulting from a search or seizure of materials in violation of the Act. Id. § 2000aa-6. This cause of action is available against the United States, against a State (if the State has

[7]The PPA also provides protection to "documentary materials, other than work product materials," which are not themselves intended for publication but which are "possessed . . . in connection with a purpose to disseminate" a public communication. 42 U.S.C. § 2000aa(b).

waived sovereign immunity), or against "any other governmental unit." Id. § 2000aa-6(a)(1). A cause of action is available against the officers or employees of a State only if the State has not waived its sovereign immunity. Id. 2000aa-6(a)2).[8] The Act provides that "[i]t shall be a complete defense to a civil action [against a government officer or employee] that the officer had a reasonable good faith belief in the lawfulness of his conduct." 42 U.S.C. § 2000aa-6(b). The district court here granted summary judgement for the officers, holding them entitled to the good faith defense due to their reliance on a warrant.

We hold instead that we lack subject matter jurisdiction over defendant officers under the PPA. The statute provides:

---

[8]Section 2000aa-6(a) reads in full:

> **Civil actions by aggrieved persons**
> **(a) Right of action**
> A person aggrieved by a search for or seizure of materials in violation of this chapter shall have a civil cause of action for damages for such search or seizure--
> (1) against the United States, against a State which has waived its sovereign immunity under the Constitution to a claim for damages resulting from a violation of this chapter, or against any other governmental unit, all of which shall be liable for violations of this chapter by their officers or employees while acting within the scope or under color of their office or employment; and
> (2) against an officer or employee of a State who has violated this chapter while acting within the scope or under color of his office or employment, if such State has not waived its sovereign immunity as provided in paragraph (1).

42 U.S.C. 2000aa-6(a).

> The remedy provided by [section 2000aa-6(a)(1)] against the United States, a State, or any other governmental unit is exclusive of any other civil action or proceeding for conduct constituting a violation of this chapter, against the officer or employee whose violation gave rise to the claim, or against the estate of such officer or employee.

Id. § 2000aa-6(d). Thus, an action under the PPA may only be brought against the governmental entity, unless the *state* has not waived sovereign immunity in which event *state* employees may be sued. Id. § 2000aa-6(a)(2). The PPA by its terms does not authorize a suit against *municipal* officers or employees in their individual capacities. The statute therefore provides no cause of action against these defendants. Although the parties stipulated below to subject-matter jurisdiction, "no action of the parties can confer subject-matter jurisdiction upon a federal court," Insurance Corp. of Ireland v. Compagnie des Bauxites de Guinee, 456 U.S. 694, 702 (1982). We dismiss the PPA claim for lack of subject-matter jurisdiction.

V

Electronic Communications Privacy Act

Plaintiffs claim that the seizure of the e-mail on the bulletin board violated the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2711.

Title II of the ECPA, id. §§ 2701-2711, bars unauthorized access to stored electronic communications. Section 2701 provides criminal penalties for whoever

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.

Id. § 2701(a). In addition to criminal penalties, the ECPA provides a civil cause of action for "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter." Id. § 2707(a). However, "[a] good faith reliance on . . . a court warrant or order . . . is a complete defense to any civil or criminal action brought under this chapter or any other law." Id. § 2707(e).

Plaintiffs contend that by seizing the e-mail and dismantling the bulletin board, the officers "obtain[ed] . . . or prevent[ed] authorized access to a[n] . . . electronic communication while it is in electronic storage" within the meaning of section 2701(a).[9] This claim raises a question of first impression in this or any

[9]We note that section 2703 establishes the requirements for governmental access to the contents of electronic communications held in electronic storage. 18 U.S.C. § 2703 (see note 11 *infra*). The State disclaimed any interest in the contents of the seized e-mail and did not seek forfeiture of the e-mail. Defendant officers also disclaim any such interest. Plaintiffs have not alleged that the officers have attempted to access or read the seized e-mail. The gravamen of the complaint is not unauthorized governmental access to the contents of the e-mail, but seizure of the e-mail and its delivery system which prevented access by the intended recipients.

circuit. There are few cases interpreting the reach of the substantive provisions of the ECPA or applying the good faith defense to violations of Title II of the ECPA, although a body of decisions does address the parallel good faith defense in Title I of the ECPA, 18 U.S.C. § 2520(d).[10] See, e.g., Heggy v. Heggy, 944 F.2d 1537, 1541-42 (10th Cir. 1991); Halperin v. Kissinger, 807 F.2d 180, 183-88 (D.C. Cir. 1986); Campiti v. Walonis, 611 F.2d 387, 394-95 (1st Cir. 1979).

Plaintiffs rely heavily on the decision in Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432 (W.D.Tex. 1993), aff'd, 36 F.3d 457 (5th Cir. 1994), which contains the most extensive discussion of the substantive provisions of the ECPA we have found. In that case, federal law enforcement officers sought a sensitive computer document stolen by computer hackers as well as evidence of related codebreaking activity. The officers had reason to believe that a suspect employed by Steve Jackson Games may have uploaded such documents to the company's computer bulletin board, which the suspect used and helped operate. No illegal activity by the company itself was alleged. The officers obtained a warrant to seize a variety of computer files and documents

[10]The earlier version of Title I of the ECPA is commonly referred to as part of Title III of the Omnibus Crime Control and Safe Streets Act. In their First Amended Complaint, plaintiffs also alleged a claim for illegal interception of electronic communications under Title I of the ECPA, 18 U.S.C. §§ 2510-2521. Title I amended Title III of the Omnibus Crime Control and Safe Streets Act governing the use of wiretapping. The district court held that the seizure here did not constitute an "interception" and granted summary judgment to the officers on that claim. Plaintiffs do not appeal on that issue.

from the company's bulletin board. The trial court found that, despite their denials, Secret Service personnel did in fact read all electronic communications seized, including private e-mail not mentioned in the search warrant or affidavit, and also deleted some of the seized files. The court held that the Secret Service's conduct with respect to the private e-mail failed to comply with the requirements of Title II of the ECPA relating to the disclosure of the contents of stored electronic communications, 18 U.S.C. § 2703. The court also declined to find the defendants entitled to a good faith defense for their reliance on the search warrant. Although the Title II issue was not appealed, the circuit court in its discussion of other issues on appeal referred approvingly to the district court's conclusion "that Title II of the ECPA clearly applies to the conduct of the Secret Service." Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

We do not find this scant precedent helpful. The circumstances here are far different from those in Steve Jackson Games. Most centrally, that case involved both a seizure of electronic communications and the subsequent review, reading, and deletion of files in electronic storage. The court focused on the provisions of section 2703, which establishes the procedures for government access to "the contents of an electronic communication."[11] We assume without deciding that an

[11]Titled, "Requirements for governmental access," section 2703 reads:
(continued...)

additional warrant in compliance with section 2703 would have been required for the law enforcement officials in the instant case to gain access to the *contents* of the seized e-mail. Plaintiffs have not alleged that the officers attempted to access or read the seized e-mail, and the officers disclaimed any interest in doing so. We are therefore faced with the entirely distinct question of whether an *incidental seizure* of electronic communications, standing alone, is a violation of the ECPA. Section 2703 does not appear to address this situation.[12]

---

[11](...continued)

> (a) Contents of electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the *contents* of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant . . . . A governmental entity may require the disclosure by a provider of electronic communications services of the *contents* of an electronic communication that has been in electronic storage . . . for more than one hundred and eighty days by the means available under subsection (b) . . . .
>
> (b) Contents of electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the *contents* of any electronic communication . . . --
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant . . . .

18 U.S.C. § 2703 (emphasis added).

[12]The various provisions of section 2703 refer repeatedly to the procedure by which the government may require a service provider to disclose communications or information of a subscriber or customer. The section provides a mechanism for a service provider to contest such a requirement, § 2703(d), and shields the service provider from liability for cooperating with the government pursuant to a court order, § 2703(e). Steve Jackson Games involved the seizure and subsequent search of e-mail from a bulletin board where the owner of the bulletin board was not a suspect in the crime. Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 436 (continued...)

We assume without deciding that plaintiffs have described conduct which constitutes a violation of section 2701, that is, that the officers "intentionally access[ed] without authorization a facility through which an electronic communication service is provided . . . and thereby . . . prevent[ed] authorized access to a wire or electronic communication while it [was] in electronic storage in such a system." 18 U.S.C. § 2701(a).[13] We further accept as true plaintiffs' assertion that a reasonable officer with the computer skills of defendant officers should have known that seizure of computer hardware would result in the seizure and disruption of e-mail. Nevertheless, we hold that the officers were entitled to summary judgment because they qualify for the statutory good faith defense as a matter of law.

Plaintiffs suggest that the officers could have made a lawful seizure of the electronically stored communications only by satisfying one of the listed

---

[12](...continued)
n.4 (W.D. Texas 1993), aff'd, 36 F.3d 457 (5th Cir. 1994). Here, the provider of the bulletin board was himself the target of the investigation, and the computer equipment storing the electronic communications was an instrumentality of the crime subject to seizure pursuant to a valid warrant.

[13]We note it is unclear whether this section was intended to apply to the sort of law enforcement activities involved here. Cf. State Wide Photocopy Corp. v. Tokai Fin. Servs., Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995) ("[I]t appears that the ECPA was primarily designed to provide a cause of action against computer hackers, (i.e., electronic trespassers)."). It is also unclear whether the term "access" encompasses the simple physical dismantling of the operating hardware.

exceptions to liability under section 2701 of the ECPA.[14] The exceptions listed contemplate that no liability attaches for "obtain[ing], alter[ing] or prevent[ing] authorized access to a . . . electronic communication," § 2701(a), if such disruption is incident to the government's access to the contents through the procedures for disclosing, § 2703, copying, § 2704, or intercepting, § 2518. In short, these exceptions all excuse government officers from liability based upon a required showing to a magistrate that the intrusive activity is necessary for a law enforcement purpose.

In addition to the enumerated exceptions, however, the statute contains the general good faith defense of section 2707(e) for reliance on a warrant. The officers relied on the warrant to seize the computer equipment, and the seizure of the stored electronic communications was incidental to the execution of the warrant. To be in good faith, the officers' reliance must have been objectively reasonable. Malley v. Briggs, 475 U.S. at 344-45. We have already concluded in our discussion of plaintiffs' Fourth Amendment claim that the warrant was valid

---

[14]Section 2701(c) reads:

> Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized--
>
> (1) by the person or entity providing a wire or electronic communications service;
>
> (2) by a user of that service with respect to a communication of or intended for that user; or
>
> (3) in section 2703, 2704 or 2518 of this title.

and encompassed the computer equipment. The officers' reliance on the warrant was therefore objectively reasonable.

Finally, plaintiffs contend the officers are not entitled to a good faith defense because they did not inform the magistrate of the possible existence of the stored electronic communications. We have held in our discussion of plaintiffs' constitutional claim that plaintiffs' inference of subjective bad faith in the officers' omission of information from the affidavit does not eliminate the officers' ability to rely on a valid warrant supported by probable cause. The plaintiffs have not persuaded us the statute imposes a requirement stricter than the Fourth Amendment in this respect. To the extent plaintiffs' contention is based on their view that the warrant must contain probable cause to seize the contents independent of the probable cause supporting the seizure of the computer, we have likewise concluded otherwise. The officers established a good faith defense as a matter of law.[15]

[15]We reiterate that we do not address here any potential statutory liability for failure to promptly copy or return stored electronic communications pursuant to a proper request to do so.

VI

Conclusion

We hold that the officers' reliance on a valid warrant entitled them to qualified immunity on plaintiffs' Fourth Amendment claim, and established a good faith defense under the ECPA.[16] We also hold that we lack subject matter jurisdiction over plaintiffs' asserted claim against the officers under the PPA. We **AFFIRM** the district court's entry of summary judgment for the officers.

[16]Although we have determined here that plaintiffs failed to allege conduct which created constitutional or statutory liability, we note that salutary benefits may accrue from a practice in the application for warrants of informing magistrates as fully as practicable of the officer's knowledge of the possible presence of publication materials or equipment for electronic storage or communication. Other cases may present closer questions of the applicability of required statutory procedures. Sufficient information will enable magistrates to set bounds which will minimize the potential for liability arising out of the initial search and seizure, or the post-seizure disposition of seized materials.